

4T
Translation09/446525
PATENT COOPERATION TREATY

PCT

2761

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

2766
RECEIVED
JAN 23 1999
IPC 270 MILL ROOM

Applicant's or agent's file reference 10F044	FOR FURTHER ACTION See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)	
International application No. PCT/JP98/02915	International filing date (day/month/year) 30 June 1998 (30.06.1998)	Priority date (day/month/year) 30 June 1997 (30.06.1997)
International Patent Classification (IPC) or national classification and IPC G09C 1/00, H04L 9/06		
Applicant NIPPON TELEGRAPH AND TELEPHONE CORPORATION		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.
2. This REPORT consists of a total of 4 sheets, including this cover sheet.
- ☐ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

These annexes consist of a total of _____ sheets.

3. This report contains indications relating to the following items:

- I ☒ Basis of the report
- II ☐ Priority
- III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- IV ☐ Lack of unity of invention
- V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- VI ☐ Certain documents cited
- VII ☐ Certain defects in the international application
- VIII ☐ Certain observations on the international application

Date of submission of the demand 08 December 1998 (08.12.1998)	Date of completion of this report 24 February 1999 (24.02.1999)
Name and mailing address of the IPEA/JP Japanese Patent Office, 4-3 Kasumigaseki 3-chome Chiyoda-ku, Tokyo 100-8915, Japan Facsimile No.	Authorized officer Telephone No. (81-3) 3581 1101

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/JP98/02915

I. Basis of the report

1. With regard to the **elements** of the international application:*

- ☒ the international application as originally filed
- ☐ the description:
 pages _____, as originally filed
 pages _____, filed with the demand
 pages _____, filed with the letter of _____
- ☐ the claims:
 pages _____, as originally filed
 pages _____, as amended (together with any statement under Article 19
 pages _____, filed with the demand
 pages _____, filed with the letter of _____
- ☐ the drawings:
 pages _____, as originally filed
 pages _____, filed with the demand
 pages _____, filed with the letter of _____
- ☐ the sequence listing part of the description:
 pages _____, as originally filed
 pages _____, filed with the demand
 pages _____, filed with the letter of _____

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.

These elements were available or furnished to this Authority in the following language _____ which is:

- ☐ the language of a translation furnished for the purposes of international search (under Rule 23.1(b)).
- ☐ the language of publication of the international application (under Rule 48.3(b)).
- ☐ the language of the translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

- ☐ contained in the international application in written form.
- ☐ filed together with the international application in computer readable form.
- ☐ furnished subsequently to this Authority in written form.
- ☐ furnished subsequently to this Authority in computer readable form.
- ☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.
- ☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. ☐ The amendments have resulted in the cancellation of:

- ☐ the description, pages _____
- ☐ the claims, Nos. _____
- ☐ the drawings, sheets/fig _____

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).**

* Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rule 70.16 and 70.17).

** Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/JP 98/02915

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement**1. Statement**

Novelty (N)	Claims	1-13	YES
	Claims		NO
Inventive step (IS)	Claims	1-13	YES
	Claims		NO
Industrial applicability (IA)	Claims	1-13	YES
	Claims		NO

2. Citations and explanations

Claims 1 to 13

Document 1: WO, 97/09705, A1 (Mitsubishi Electric Corp.), March 13, 1997 (13.03.97), full text, Fig. 1 to 29

Document 1 is a document that illustrates the general technical level in the technical field and describes a technique that changes the structure of the sub-converter capable of partial parallel processing of the input data to enable high-speed data conversion having excellent differential probabilities. However, None of the documents listed in the international search report nor the documents newly cited in the international preliminary examination report describes or suggests a specific structure for a rounding processor and the structure for a nonlinear function unit which are described in the claims.

Claims 1 to 13

Document 2: Mitsuru Matsui, "Provable Safety of Differential Decoding and Linear Decoding of Block Cipher (in Japanese)", Preprint of the 18th Symposium on Information Theories and their Applications, The Institute of Information Theories and their Applications, Vol. 1 of 2, October 1995 (10.95), pp. 175-178

Document 2 is a document indicating the general technical level in the technical field and describes a technique that can change the position of the F function and parallel process as a block cipher that implements verifiable security for differential decoding and linear decoding, and construct an entire structure by deriving a recursive structure for the function and using a smaller computational unit. However, none of the documents listed in the international search report, nor the documents newly cited in the international preliminary examination report describes or suggests specific structures for the rounding processor and the nonlinear function unit described in the claims.

Claims 1 to 13

Document 3: Mitsuru Matsui, "Practical Block Cipher Having Provable Safety of Differential Decoding and Linear Decoding (in Japanese)", Symposium on Cipher and Information Security, SCIS96, Information Security Research Special Committee of IEICE, January 1996 (01.96) SCIS96-4C

Document 3 is a document indicating the general technical level in the technical field and describes a design technique for a block cipher that has verifiable security for differential decoding and linear decoding. However, none of the documents listed in the international search report nor the documents newly cited in the international preliminary examination report describes or suggests specific structures for the rounding processor and the nonlinear function unit described in the claims.

Claims 1 to 13

Document 14: JP, 9-54547, A (NEC Corp.), February 25, 1997 (25.02.97), full text, Fig. 1 to 11

Document 4 is a document indicating the general technical level in the technical field and describes an improved technique to build a data conversion means to implement a high level of security against attacks in differential decoding and linear decoding. However, none of the documents listed in the international search report nor the documents newly cited in the international preliminary examination report describes or suggests specific structures for the rounding processor and the nonlinear function unit described in the claims.

Claims 1 to 13

Document 5: Masato Kanda, et al., "Structure of Round Function Using a Little S-box (Part 1) (in Japanese)," Technical Research Report of IEICE (ISEC97 14-22), Vol. 97, No. 181, July 18, 1997 (18.07.97), pp. 41-52.

Document 5 is a document indicating the general technical level in the technical field and describes a technique to build a rounding function using a small number of S-boxes based on the evaluation standard of the verifiable security for decoding block ciphers represented by differential decoding and linear decoding. None of the documents listed in the international search report nor the documents newly cited in the international preliminary examination report describes specific structures for the rounding processor and the nonlinear function unit described in the claims.

REC'D 26 MAR 1999

WIPO PCT

PCT

国際予備審査報告

(法第12条、法施行規則第56条)
[PCT36条及びPCT規則70]

出願人又は代理人 の書類記号 10F044	今後の手続きについては、国際予備審査報告の送付通知(様式PCT/ IPEA/416)を参照すること。	
国際出願番号 PCT/J P 98/02915	国際出願日 (日.月.年) 30.06.98	優先日 (日.月.年) 30.06.97
国際特許分類(IPC) Int. Cl ⁸ G09C1/00, H04L9/06		
出願人(氏名又は名称) 日本電信電話株式会社		

1. 国際予備審査機関が作成したこの国際予備審査報告を法施行規則第57条(PCT36条)の規定に従い送付する。
2. この国際予備審査報告は、この表紙を含めて全部で 4 ページからなる。 <input type="checkbox"/> この国際予備審査報告には、附属書類、つまり補正されて、この報告の基礎とされた及び/又はこの国際予備審査機関に対してした訂正を含む明細書、請求の範囲及び/又は図面も添付されている。 (PCT規則70.16及びPCT実施細則第607号参照) この附属書類は、全部で ページである。
3. この国際予備審査報告は、次の内容を含む。 I <input checked="" type="checkbox"/> 国際予備審査報告の基礎 II <input type="checkbox"/> 優先権 III <input type="checkbox"/> 新規性、進歩性又は産業上の利用可能性についての国際予備審査報告の不作成 IV <input type="checkbox"/> 発明の単一性の欠如 V <input checked="" type="checkbox"/> PCT35条(2)に規定する新規性、進歩性又は産業上の利用可能性についての見解、それを裏付けるための文献及び説明 VI <input type="checkbox"/> ある種の引用文献 VII <input type="checkbox"/> 国際出願の不備 VIII <input type="checkbox"/> 国際出願に対する意見

国際予備審査の請求書を受理した日 08.12.98	国際予備審査報告を作成した日 24.02.98	
名称及びあて先 日本国特許庁(IPEA/J P) 郵便番号100-8915 東京都千代田区霞が関三丁目4番3号	特許庁審査官(権限のある職員) 青木 重徳 電話番号 03-3581-1101 内線 3538	5 J 4229

I. 国際予備審査報告の基礎

1. この国際予備審査報告は下記の出願書類に基づいて作成された。(法第6条(PCT14条)の規定に基づく命令に
 応答するために提出された差し替え用紙は、この報告書において「出願時」とし、本報告書には添付しない。
 PCT規則70.16, 70.17)

☒ 出願時の国際出願書類

- ☐ 明細書 第 _____ ページ、 出願時に提出されたもの
 明細書 第 _____ ページ、 国際予備審査の請求書と共に提出されたもの
 明細書 第 _____ ページ、 _____ 付の書簡と共に提出されたもの
- ☐ 請求の範囲 第 _____ 項、 出願時に提出されたもの
 請求の範囲 第 _____ 項、 PCT19条の規定に基づき補正されたもの
 請求の範囲 第 _____ 項、 国際予備審査の請求書と共に提出されたもの
 請求の範囲 第 _____ 項、 _____ 付の書簡と共に提出されたもの
- ☐ 図面 第 _____ ページ/図、 出願時に提出されたもの
 図面 第 _____ ページ/図、 国際予備審査の請求書と共に提出されたもの
 図面 第 _____ ページ/図、 _____ 付の書簡と共に提出されたもの
- ☐ 明細書の配列表の部分 第 _____ ページ、 出願時に提出されたもの
 明細書の配列表の部分 第 _____ ページ、 国際予備審査の請求書と共に提出されたもの
 明細書の配列表の部分 第 _____ ページ、 _____ 付の書簡と共に提出されたもの

2. 上記の出願書類の言語は、下記に示す場合を除くほか、この国際出願の言語である。

上記の書類は、下記の言語である _____ 語である。

- ☐ 国際調査のために提出されたPCT規則23.1(b)にいう翻訳文の言語
☐ PCT規則48.3(b)にいう国際公開の言語
☐ 国際予備審査のために提出されたPCT規則55.2または55.3にいう翻訳文の言語

3. この国際出願は、ヌクレオチド又はアミノ酸配列を含んでおり、次の配列表に基づき国際予備審査報告を行った。

- ☐ この国際出願に含まれる書面による配列表
☐ この国際出願と共に提出されたフレキシブルディスクによる配列表
☐ 出願後に、この国際予備審査(または調査)機関に提出された書面による配列表
☐ 出願後に、この国際予備審査(または調査)機関に提出されたフレキシブルディスクによる配列表
☐ 出願後に提出した書面による配列表が出願時における国際出願の開示の範囲を超える事項を含まない旨の陳述書の提出があった
☒ 書面による配列表に記載した配列とフレキシブルディスクによる配列表に記載した配列が同一である旨の陳述書の提出があった。

4. 補正により、下記の書類が削除された。

- ☐ 明細書 第 _____ ページ
☐ 請求の範囲 第 _____ 項
☐ 図面 図面の第 _____ ページ/図

5. ☐ この国際予備審査報告は、補充欄に示したように、補正が出願時における開示の範囲を越えてされたものと認められるので、その補正がされなかったものとして作成した。(PCT規則70.2(c) この補正を含む差し替え用紙は上記1.における判断の際に考慮しなければならず、本報告に添付する。)

V. 新規性、進歩性又は産業上の利用可能性についての法第12条(PCT35条(2))に定める見解、それを裏付ける文献及び説明

1. 見解

新規性 (N)	請求の範囲	1-13	有
	請求の範囲		無
進歩性 (IS)	請求の範囲	1-13	有
	請求の範囲		無
産業上の利用可能性 (IA)	請求の範囲	1-13	有
	請求の範囲		無

2. 文献及び説明 (PCT規則70.7)

請求の範囲 1-13

文献1: W0, 97/09705, A1 (三菱電機株式会社)

13.3月.1997 (13.03.97) 全文, 第1-29図

は、当該技術分野における一般的技術水準を示す文献であって、差分確率の優れた高速なデータ変換を可能とするために、入力データを部分的に並列処理できるように副変換処理部の構成を変更する技術が記載されているが、各請求の範囲に記載されている具体的なラウンド処理部の構成や非線形関数部の構成については、国際調査報告書で列記した文献、および国際予備審査報告書にて新たに引用した文献のいずれにも、記載も示唆もされていない。

請求の範囲 1-13

文献2: 松井充, “ブロック暗号の差分解読法と線形解読法に対する証明可能安全性について”,

第18回情報理論とその応用シンポジウム予稿集,

情報理論とその応用学会, Vol. 1 of 2, 10月.1995 (10.95) p. 175-178

は、当該技術分野における一般的技術水準を示す文献であって、差分解読法と線形解読法に対する証明可能安全性を実現するブロック暗号として、F関数の位置を変更し、並列処理を可能にすると共に、このF関数に再帰構造を導入し、より小さな演算単位を用いて全体を構成する技術が記載されているが、各請求の範囲に記載されている具体的なラウンド処理部の構成や非線形関数部の構成については、国際調査報告書で列記した文献、および国際予備審査報告書にて新たに引用した文献のいずれにも、記載も示唆もされていない。

請求の範囲 1-13

文献3: 松井充, “差分解読法と線形解読法に対する証明可能安全性をもつ実用ブロック暗号”,

暗号と情報セキュリティシンポジウムASCIS96講演論文集,

電子情報通信学会情報セキュリティ研究専門委員会, 1月.1996 (01.96) SCIS96-4C

は、当該技術分野における一般的技術水準を示す文献であって、差分解読法および線形解読法に対して証明可能安全性をもつブロック暗号の設計技術が記載されているが、各請求の範囲に記載されている具体的なラウンド処理部の構成や非線形関数部の構成については、国際調査報告書で列記した文献、および国際予備審査報告書にて新たに引用した文献のいずれにも、記載も示唆もされていない。

補充欄 (いずれかの欄の大きさが足りない場合に使用すること)

第 V. 5 欄の続き

請求の範囲 1-13

文献4: JP, 9-54547, A (日本電気株式会社)

25.2月.1997 (25.02.97) 全文, 第1-11図

は、当該技術分野における一般的技術水準を示す文献であって、差分解読法や線形解読法などの攻撃に対して高い安全性を実現するために、データ変換手段の改良構成技術が記載されているが、各請求の範囲に記載されている具体的なラウンド処理部の構成や非線形関数部の構成については、国際調査報告書で列記した文献、および国際予備審査報告書にて新たに引用した文献のいずれにも、記載も示唆もされていない。

請求の範囲 1-13

文献5: 神田雅透 他, “少数のS-boxを用いたラウンド関数の構成について(その1)”,

電子情報通信学会技術研究報告 (ISEC97 14~22),

Vol. 97, No. 181, 18.7月.1997 (18.07.97) p. 41-52

は、当該技術分野における一般的技術水準を示す文献であって、差分解読法や線形解読法に代表されるブロック暗号に対する解読法に対する証明可能安全性の評価基準を基に、少数のS-boxを用いてラウンド関数を構成する技術が記載されているが、各請求の範囲に記載されている具体的なラウンド処理部の構成や非線形関数部の構成については、国際調査報告書で列記した文献、および国際予備審査報告書にて新たに引用した文献のいずれにも、記載も示唆もされていない。

PCT

EP

US

国際調査報告

(法8条、法施行規則第40、41条)
[PCT18条、PCT規則43、44]

出願人又は代理人 の書類記号 10F044	今後の手続きについては、国際調査報告の送付通知様式(PCT/ISA/22 及び下記5を参照すること。	
国際出願番号 PCT/JP98/02915	国際出願日 (日.月.年) 30.06.98	優先日 (日.月.年) 30.06.97
出願人(氏名又は名称) 日本電信電話株式会社		

国際調査機関が作成したこの国際調査報告を法施行規則第41条(PCT18条)の規定に従い出願人に送付する。
この写しは国際事務局にも送付される。

この国際調査報告は、全部で 3 ページである。

☐ この調査報告に引用された先行技術文献の写しも添付されている。

1. ☐ 請求の範囲の一部の調査ができない(第I欄参照)。

2. ☐ 発明の単一性が欠如している(第II欄参照)。

3. ☐ この国際出願は、ヌクレオチド及び/又はアミノ酸配列リストを含んでおり、次の配列リストに基づき国際調査を行った。

☐ この国際出願と共に提出されたもの

☐ 出願人がこの国際出願とは別に提出したもの

☐ しかし、出願時の国際出願の開示の範囲を越える事項を含まない旨を記載した書面が添付されていない

☐ この国際調査機関が書換えたもの

4. 発明の名称は ☒ 出願人が提出したものを承認する。
☐ 次に示すように国際調査機関が作成した。

5. 要約は ☒ 出願人が提出したものを承認する。
☐ 第III欄に示されているように、法施行規則第47条(PCT規則38.2(b))の規定により国際調査機関が作成した。出願人は、この国際調査報告の発送の日から1カ月以内にこの国際調査機関に意見を提出することができる。

6. 要約書とともに公表される図は、
第 4 図とする。 ☒ 出願人が示したとおりである。 ☐ なし
☐ 出願人は図を示さなかった。
☐ 本図は発明の特徴を一層よく表している。

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl.[°] G09C1/00, H04L9/06

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl.[°] G09C1/00, H04L9/06

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1922-1996年
 日本国公開実用新案公報 1971-1998年
 日本国登録実用新案公報 1994-1998年
 日本国実用新案登録公報 1996-1998年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
A	WO, 98/09705, A1 (三菱電機株式会社) 13.3月.1997(13-03.97) 全文, 第1-29図 & AU, 6629396, A1 & NO, 972052, A & EP, 790595, A1	1-13
A	松井充, ブロック暗号の差分解読法と線形解読法に対する証明可能安全性について, 第18回情報理論とその応用シンポジウム予稿集, 情報理論とその応用学会, Vol. 1 of 2 10月. 1995(10.95) p. 175-178	1-13

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの
 「E」 先行文献ではあるが、国際出願日以後に公表されたもの
 「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)
 「O」 口頭による開示、使用、展示等に言及する文献
 「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
 「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
 「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
 「&」 同一パテントファミリー文献

国際調査を完了した日

17.09.98

国際調査報告の発送日

29.09.98

国際調査機関の名称及びあて先

日本国特許庁 (ISA/J P)
 郵便番号100-8915
 東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

青木 重徳

5 J

4229

電話番号 03-3581-1101 内線 3538

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
A	松井充 他, 差分解読法と線形解読法に対する証明可能安全性をもつ実用ブロック暗号, 暗号と情報セキュリティシンポジウムSCIS96講演論文集, 電子情報通信学会情報セキュリティ研究専門委員会, 1月. 1996 (01. 96) SCIS96-4C	1-13
A	JP, 9-54547, A (日本電気株式会社) 25. 2月. 1997 (25. 02. 97) 全文, 第1-11図 (ファミリーなし)	1-13
P, A	神田雅透 他, 少数のS-boxを用いたラウンド関数の構成について(その1), 電子情報通信学会技術研究報告 (ISEC97 14-22), Vol. 97, No. 181, 18. 7月. 1997 (18. 07. 97) p. 41-52	1-13

PCT

REQUEST

The undersigned requests that the present international application be processed according to the Patent Cooperation Treaty.

For receiving Office use only

International Application No. PCT/JP98/02915

International Filing Date 30 June, 1998

Name of receiving Office and "PCT International Application"

Applicant's or agent's file reference
(if desired) (12 characters maximum) 10F044

Box No. I TITLE OF INVENTION
"CRYPTOGRAPHIC DEVICE"

Box No. II APPLICANT

Name and address: (Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (i.e. country) of residence if no State of residence is indicated below.)

NIPPON TELEGRAPH AND
TELEPHONE CORPORATION

19-2, Nishi-Shinjuku 3-chome, Shinjuku-ku,
Tokyo 163-8019 Japan

☐ This person is also inventor.

Telephone No. 03-5353-4343

Facsimile No. 03-5353-5518

Teleprinter No.

State (i.e. country) of nationality: JAPAN

State (i.e. country) of residence: JAPAN

This person is applicant for the purposes of: ☐ all designated States ☒ all designated States except the United States of America ☐ the United States of America only ☐ the States indicated in the Supplemental Box

Box No. III FURTHER APPLICANT(S) AND/OR (FURTHER) INVENTOR(S)

Name and address: (Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (i.e. country) of residence if no State of residence is indicated below.)

KANDA Masayuki

C/O NIPPON TELEGRAPH AND
TELEPHONE CORPORATION,

20-2 Nishi-Shinjuku 3-chome, Shinjuku-ku,
Tokyo 163-1419 Japan

This person is:

☐ applicant only

☒ applicant and inventor

☐ inventor only (If this check-box is marked, do not fill in below.)

State (i.e. country) of nationality: JAPAN

State (i.e. country) of residence: JAPAN

This person is applicant for the purposes of: ☐ all designated States ☐ all designated States except the United States of America ☒ the United States of America only ☐ the States indicated in the Supplemental Box

☒ Further applicants and/or (further) inventors are indicated on a continuation sheet.

Box No. IV AGENT OR COMMON REPRESENTATIVE; OR ADDRESS FOR CORRESPONDENCE

The person identified below is hereby/has been appointed to act on behalf of the applicant(s) before the competent International Authorities as: ☒ agent ☐ common representative

Name and address: (Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country.)

6615 Patent Attorney KUSANO Takashi

10064 Patent Attorney INAGAKI Minoru

Sagami Bldg., 2-21, Shinjuku 4-chome,

Shinjuku-ku, Tokyo 160-0022 Japan

Telephone No. 03-3350-6456

Facsimile No. 03-5379-7396

Teleprinter No.

☐ Mark this check-box where no agent or common representative is/has been appointed and the space above is used instead to indicate a special address to which correspondence should be sent.

Continuation of Box No. III FURTHER APPLICANTS AND/OR (FURTHER) INVENTORS			
<i>If none of the following sub-boxes is used, this sheet is not to be included in the request.</i>			
<p>Name and address: (Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (i.e. country) of residence if no State of residence is indicated below.)</p> <p>TAKASHIMA Youichi C/O NIPPON TELEGRAPH AND TELEPHONE CORPORATION, 20-2 Nishi-Shinjuku 3-chome, Shinjuku-ku, Tokyo 163-1419 Japan</p>		<p>This person is:</p> <p><input type="checkbox"/> applicant only</p> <p><input checked="" type="checkbox"/> applicant and inventor</p> <p><input type="checkbox"/> inventor only (If this check-box is marked, do not fill in below.)</p>	
<p>State (i.e. country) of nationality: JAPAN</p>		<p>State (i.e. country) of residence: JAPAN</p>	
<p>This person is applicant for the purposes of: <input type="checkbox"/> all designated States <input type="checkbox"/> all designated States except the United States of America <input checked="" type="checkbox"/> the United States of America only <input type="checkbox"/> the States indicated in the Supplemental Box</p>			
<p>Name and address: (Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (i.e. country) of residence if no State of residence is indicated below.)</p> <p>AOKI Katsuhiko 5-11-5, Minami-Aoyama, Minato-ku, Tokyo 107-0062 Japan</p>		<p>This person is:</p> <p><input type="checkbox"/> applicant only</p> <p><input checked="" type="checkbox"/> applicant and inventor</p> <p><input type="checkbox"/> inventor only (If this check-box is marked, do not fill in below.)</p>	
<p>State (i.e. country) of nationality: JAPAN</p>		<p>State (i.e. country) of residence: JAPAN</p>	
<p>This person is applicant for the purposes of: <input type="checkbox"/> all designated States <input type="checkbox"/> all designated States except the United States of America <input checked="" type="checkbox"/> the United States of America only <input type="checkbox"/> the States indicated in the Supplemental Box</p>			
<p>Name and address: (Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (i.e. country) of residence if no State of residence is indicated below.)</p> <p>Matsumoto Tsutomu 13-45, Kakinokidai, Aoba-ku, Yokohama-shi, Kanagawa 227-0048 Japan</p>		<p>This person is:</p> <p><input type="checkbox"/> applicant only</p> <p><input checked="" type="checkbox"/> applicant and inventor</p> <p><input type="checkbox"/> inventor only (If this check-box is marked, do not fill in below.)</p>	
<p>State (i.e. country) of nationality: JAPAN</p>		<p>State (i.e. country) of residence: JAPAN</p>	
<p>This person is applicant for the purposes of: <input type="checkbox"/> all designated States <input type="checkbox"/> all designated States except the United States of America <input checked="" type="checkbox"/> the United States of America only <input type="checkbox"/> the States indicated in the Supplemental Box</p>			
<p>Name and address: (Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (i.e. country) of residence if no State of residence is indicated below.)</p>		<p>This person is:</p> <p><input type="checkbox"/> applicant only</p> <p><input type="checkbox"/> applicant and inventor</p> <p><input type="checkbox"/> inventor only (If this check-box is marked, do not fill in below.)</p>	
<p>State (i.e. country) of nationality:</p>		<p>State (i.e. country) of residence:</p>	
<p>This person is applicant for the purposes of: <input type="checkbox"/> all designated States <input type="checkbox"/> all designated States except the United States of America <input type="checkbox"/> the United States of America only <input type="checkbox"/> the States indicated in the Supplemental Box</p>			
<p><input type="checkbox"/> Further applicants and/or (further) inventors are indicated on another continuation sheet.</p>			

Box No.V DESIGNATION OF STATES

The following designations are hereby made under Rule 4.9(a) (mark the applicable check-boxes; at least one must be marked):

Regional Patent

- ☐ AP **ARIPO Patent:** KE Kenya, LS Lesotho, MW Malawi, SD Sudan, SZ Swaziland, UG Uganda, and any other State which is a Contracting State of the Harare Protocol and of the PCT
- ☐ EA **Eurasian Patent:** AM Armenia, AZ Azerbaijan, BY Belarus, KG Kyrgyzstan, KZ Kazakstan, MD Republic of Moldova, RU Russian Federation, TJ Tajikistan, TM Turkmenistan, and any other State which is a Contracting State of the Eurasian Patent Convention and of the PCT
- ☒ EP **European Patent:** AT Austria, BE Belgium, CH and LI Switzerland and Liechtenstein, DE Germany, DK Denmark, ES Spain, FI Finland, FR France, GB United Kingdom, GR Greece, IE Ireland, IT Italy, LU Luxembourg, MC Monaco, NL Netherlands, PT Portugal, SE Sweden, and any other State which is a Contracting State of the European Patent Convention and of the PCT
- ☐ OA **OAPI Patent:** BF Burkina Faso, BJ Benin, CF Central African Republic, CG Congo, CI Côte d'Ivoire, CM Cameroon, GA Gabon, GN Guinea, ML Mali, MR Mauritania, NE Niger, SN Senegal, TD Chad, TG Togo, and any other State which is a member State of OAPI and a Contracting State of the PCT (if other kind of protection or treatment desired, specify on dotted line)

National Patent (if other kind of protection or treatment desired, specify on dotted line):

- | | |
|---|---|
| <input type="checkbox"/> AL Albania | <input type="checkbox"/> LU Luxembourg |
| <input type="checkbox"/> AM Armenia | <input type="checkbox"/> LV Latvia |
| <input type="checkbox"/> AT Austria | <input type="checkbox"/> MD Republic of Moldova |
| <input type="checkbox"/> AU Australia | <input type="checkbox"/> MG Madagascar |
| <input type="checkbox"/> AZ Azerbaijan | <input type="checkbox"/> MK The former Yugoslav Republic of Macedonia |
| <input type="checkbox"/> BA Bosnia and Herzegovina | <input type="checkbox"/> MN Mongolia |
| <input type="checkbox"/> BB Barbados | <input type="checkbox"/> MW Malawi |
| <input type="checkbox"/> BG Bulgaria | <input type="checkbox"/> MX Mexico |
| <input type="checkbox"/> BR Brazil | <input type="checkbox"/> NO Norway |
| <input type="checkbox"/> BY Belarus | <input type="checkbox"/> NZ New Zealand |
| <input checked="" type="checkbox"/> CA Canada | <input type="checkbox"/> PL Poland |
| <input type="checkbox"/> CH and LI Switzerland and Liechtenstein | <input type="checkbox"/> PT Portugal |
| <input type="checkbox"/> CN China | <input type="checkbox"/> RO Romania |
| <input type="checkbox"/> CU Cuba | <input type="checkbox"/> RU Russian Federation |
| <input type="checkbox"/> CZ Czech Republic | <input type="checkbox"/> SD Sudan |
| <input type="checkbox"/> DE Germany | <input type="checkbox"/> SE Sweden |
| <input type="checkbox"/> DK Denmark | <input type="checkbox"/> SG Singapore |
| <input type="checkbox"/> EE Estonia | <input type="checkbox"/> SI Slovenia |
| <input type="checkbox"/> ES Spain | <input type="checkbox"/> SK Slovakia |
| <input type="checkbox"/> FI Finland | <input type="checkbox"/> TJ Tajikistan |
| <input type="checkbox"/> GB United Kingdom | <input type="checkbox"/> TM Turkmenistan |
| <input type="checkbox"/> GE Georgia | <input type="checkbox"/> TR Turkey |
| <input type="checkbox"/> HU Hungary | <input type="checkbox"/> TT Trinidad and Tobago |
| <input type="checkbox"/> IL Israel | <input type="checkbox"/> UA Ukraine |
| <input type="checkbox"/> IS Iceland | <input type="checkbox"/> UG Uganda |
| <input type="checkbox"/> JP Japan | <input checked="" type="checkbox"/> US United States of America |
| <input type="checkbox"/> KE Kenya | <input type="checkbox"/> UZ Uzbekistan |
| <input type="checkbox"/> KG Kyrgyzstan | <input type="checkbox"/> VN Viet Nam |
| <input type="checkbox"/> KP Democratic People's Republic of Korea | |
| <input type="checkbox"/> KR Republic of Korea | |
| <input type="checkbox"/> KZ Kazakstan | |
| <input type="checkbox"/> LC Saint Lucia | |
| <input type="checkbox"/> LK Sri Lanka | |
| <input type="checkbox"/> LR Liberia | |
| <input type="checkbox"/> LS Lesotho | |
| <input type="checkbox"/> LT Lithuania | |

Check-boxes reserved for designating States (for the purposes of a national patent) which have become party to the PCT after issuance of this sheet:

- ☐
☐
☐
☐

In addition to the designations made above, the applicant also makes under Rule 4.9(b) all designations which would be permitted under the PCT except the designation(s) of

The applicant declares that those additional designations are subject to confirmation and that any designation which is not confirmed before the expiration of 15 months from the priority date is to be regarded as withdrawn by the applicant at the expiration of that time limit. (Confirmation of a designation consists of the filing of a notice specifying that designation and the payment of the designation and confirmation fees. Confirmation must reach the receiving Office within the 15-month time limit.)

Box No. VI PRIORITY CLAIM		Further priority claims are indicated in the Supplemental Box <input type="checkbox"/>	
The priority of the following earlier application(s) is hereby claimed:			
Country (in which, or for which, the application was filed)	Filing Date (day/month/year)	Application No.	Office of filing (only for regional or international application)
item (1) Japan	30. 06. 97	173672/97	
item (2)			
item (3)			
Mark the following check-box if the certified copy of the earlier application is to be issued by the Office which for the purposes of the present international application is the receiving Office (a fee may be required): <input checked="" type="checkbox"/> The receiving Office is hereby requested to prepare and transmit to the International Bureau a certified copy of the earlier application(s) identified above as item(s): (1)			
Box No. VII INTERNATIONAL SEARCHING AUTHORITY			
Choice of International Searching Authority (ISA) (If two or more International Searching Authorities are competent to carry out the international search, indicate the Authority chosen; the two-letter code may be used): ISA / J P			
Earlier search Fill in where a search (international, international-type or other) by the International Searching Authority has already been carried out or requested and the Authority is now requested to base the international search, to the extent possible, on the results of that earlier search. Identify such search or request either by reference to the relevant application (or the translation thereof) or by reference to the search request: Country (or regional Office): Date (day/month/year): Number:			
Box No. VIII CHECK LIST			
This international application contains the following number of sheets: 1. request : 4 sheets 2. description : 17 sheets 3. claims : 3 sheets 4. abstract : 1 sheets 5. drawings : 9 sheets Total : 34 sheets		This international application is accompanied by the item(s) marked below: 1. <input checked="" type="checkbox"/> separate signed power of attorney 5. <input checked="" type="checkbox"/> fee calculation sheet 2. <input type="checkbox"/> copy of general power of attorney 6. <input type="checkbox"/> separate indications concerning deposited microorganisms 3. <input type="checkbox"/> statement explaining lack of signature 7. <input type="checkbox"/> nucleotide and/or amino acid sequence listing (diskette) 4. <input type="checkbox"/> priority document(s) identified in Box No. VI as item(s): Request for mailing Priority Document 8. <input checked="" type="checkbox"/> other (specify):	
Figure No. 4 of the drawings (if any) should accompany the abstract when it is published.			
Box No. IX SIGNATURE OF APPLICANT OR AGENT			
Next to each signature, indicate the name of the person signing and the capacity in which the person signs (if such capacity is not obvious from reading the request).			
KUSANO Takashi (Seal)			
INAGAKI Minoru (Seal)			

For receiving Office use only	
1. Date of actual receipt of the purported international application:	2. Drawings: <input type="checkbox"/> received: <input type="checkbox"/> not received:
3. Corrected date of actual receipt due to later but timely received papers or drawings completing the purported international application:	
4. Date of timely receipt of the required corrections under PCT Article 11(2):	
5. International Searching Authority specified by the applicant: ISA /	6. <input type="checkbox"/> Transmittal of search copy delayed until search fee is paid

For International Bureau use only
Date of receipt of the record copy by the International Bureau:

PATENT COOPERATION TREATY

PCT

NOTIFICATION OF ELECTION

(PCT Rule 61.2)

From the INTERNATIONAL BUREAU

To:

Assistant Commissioner for Patents
United States Patent and Trademark
Office
Box PCT
Washington, D.C.20231
ÉTATS-UNIS D'AMÉRIQUE

in its capacity as elected Office

Date of mailing: 21 October 1999 (21.10.99)	
International application No.: PCT/JP98/02915	Applicant's or agent's file reference: 10F044
International filing date: 30 June 1998 (30.06.98)	Priority date: 30 June 1997 (30.06.97)
Applicant: KANDA, Masayuki et al	

1. The designated Office is hereby notified of its election made:

☒ in the demand filed with the International preliminary Examining Authority on:
08 December 1998 (08.12.98)

☐ in a notice effecting later election filed with the International Bureau on:

2. The election ☒ was
☐ was not

made before the expiration of 19 months from the priority date or, where Rule 32 applies, within the time limit under Rule 32.2(b).

The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland Facsimile No.: (41-22) 740.14.35	Authorized officer: J. Zahra Telephone No.: (41-22) 338.83.38
---	---

定理 2 の証明 (1), (2) と同様にして, $DCP_{\max}^1 \leq 1$.

$$DCP_{\max}^2 \leq p \text{ となる.}$$

ゆえに, $DCP_{\max}^N \leq p^N (N=1), DCP_{\max}^N \leq p (N=2)$ が成り立つ.

(2) $N=3, 4, 5 (n=1)$ のとき

まず, $\Delta X_3^2 = 0$ について考える.

このとき, $X_1^2 = \Delta X_2^2 \neq 0$ でなければならぬ.
よって, $\Delta Y_2 \neq 0$ であるから, $\Delta X_1^2 = \Delta Y_2 \neq 0$ となる.
したがって,

$$DCP_{\max}^1 = \max_{\Delta Y_1 \neq 0} DP(\Delta X_1^1 \rightarrow \Delta Y_1) \cdot DP(\Delta X_2^1 \rightarrow \Delta Y_2) \leq p^2$$

となる.

さらに, $\Delta Y_3 = 0$ であるから, $\Delta X_3^2 = \Delta X_2^2 \neq 0$ となり, $DP(\Delta X_2^2 \rightarrow \Delta Y_3) \leq p$ である. また, $\Delta Y_2 \neq 0$ であるから, $\Delta X_3^2 = \Delta Y_2 \neq 0$ となり, $DP(\Delta X_3^2 \rightarrow \Delta Y_2) \leq p$ である. 以上のことから,

$$DCP_{\max}^2 = DCP_{\max}^1 \cdot DP(\Delta X_2^2 \rightarrow \Delta Y_3) \leq p^2 \cdot p = p^3$$

$$DCP_{\max}^3 = DCP_{\max}^2 \cdot DP(\Delta X_3^3 \rightarrow \Delta Y_3) \leq p^3 \cdot p = p^4$$

となる.

次に, $\Delta X_3^2 \neq 0$ についてを考える.

このとき, $\Delta X_2^2 = \Delta X_1^2, \Delta Y_2$ の少なくとも一方が 0 ではない. また, $\Delta Y_2 \neq 0$ であれば $\Delta X_2^2 \neq 0$ となり, 同様にして $\Delta X_1^2, \Delta Y_1$ の少なくとも一方が 0 ではないことが導かれる. ゆえに, $\Delta X_1 \neq 0$ である. さて, ラウンド関数 F が全単射であることに注意すれば, (1) から $\Delta X_1 = (\Delta X_1^1, 0), \Delta X_1^1 \neq 0$ のときに $DCP_{\max}^2 \leq p$ で, かつ $\Delta X_3^2 \neq 0$ になることが示される. よって,

$$DCP_{\max}^1 = DCP_{\max}^2 \cdot DP(\Delta X_3^2 \rightarrow \Delta Y_3) \leq p \cdot p = p^2$$

となる.

さらに, $\Delta Y_3 = \Delta X_2^2$ とすると $\Delta X_2^2 = 0$ となり, $DCP_{\max}^2 = DCP_{\max}^1 \leq p^2$ である. また, $\Delta X_3^2 = \Delta X_1^2 \neq 0$ となるから, $DCP_{\max}^3 = DCP_{\max}^2 \cdot DP(\Delta X_3^3 \rightarrow \Delta Y_3) \leq p^3$ である.

以上のことから,

$$DCP_{\max}^N \leq p^3 = UDP^N (N=3, 4)$$

$$DCP_{\max}^N \leq p^4 = UDP^N (N=5)$$

が成り立つ.

(3) $N=3n, 3n+1, 3n+2 (n=m+1, m \geq 1)$ のとき

$DCP_{\max}^{3n} \leq p^{3n}, DCP_{\max}^{3n+1} \leq p^{3n}, DCP_{\max}^{3n+2} \leq p^{3n+1}$ が成り立っていると仮定する. この仮定より,
 $DP(\Delta X_{3n-1}^2 \rightarrow \Delta Y_{3n-1}) = 1, DP(\Delta X_{3n-2}^2 \rightarrow \Delta Y_{3n-2}) \leq p$,
 $\Delta X_{3n-1}^2 = \Delta Y_{3n-1} = 0, \Delta X_{3n-2}^2 \neq 0, \Delta Y_{3n-2} \neq 0$ となる.

このとき,

$$DCP_{\max}^{3n} = \max_{\Delta Y_{3n-2} \neq 0} DCP_{\max}^{3n-2} \cdot DP(\Delta X_{3n-1}^2 \rightarrow \Delta Y_{3n-1})$$

$$DCP_{\max}^{3n+1} = \max_{\substack{\Delta Y_{3n-2} \neq 0 \\ \Delta Y_{3n-1} \neq 0}} \left\{ DCP_{\max}^{3n-2} \cdot DP(\Delta X_{3n-1}^2 \rightarrow \Delta Y_{3n-1}) \right. \\ \left. \times DP(\Delta X_{3n-2}^2 \rightarrow \Delta Y_{3n-2}) \right\}$$

$$DCP_{\max}^{3n+2} = \max_{\substack{\Delta Y_{3n-2} \neq 0 \\ \Delta Y_{3n-1} \neq 0}} \left\{ DCP_{\max}^{3n-2} \cdot DP(\Delta X_{3n-1}^2 \rightarrow \Delta Y_{3n-1}) \right. \\ \left. \times DP(\Delta X_{3n-2}^2 \rightarrow \Delta Y_{3n-2}) \right\}$$

である.

ここで, $\Delta X_{3n-1}^2 = 0$ であるという仮定より,
 $\Delta X_{3n-1}^2 = \Delta Y_{3n-2} \neq 0$ であるから, $DP(\Delta X_{3n-1}^2 \rightarrow \Delta Y_{3n-1}) \leq p$ となる.

さらに, $\Delta Y_{3n} = \Delta X_{3n-2}^2 \neq 0$ とすると, $\Delta X_{3n-1}^2 = 0$ となり, $DP(\Delta X_{3n-1}^2 \rightarrow \Delta Y_{3n}) \cdot DP(\Delta X_{3n-2}^2 \rightarrow \Delta Y_{3n-2}) \leq p$ である. また, このとき $\Delta X_{3n-2}^2 = \Delta X_{3n-2}^2 \neq 0$ となるので, $\prod_{i=1}^{3n-2} DP(\Delta X_i^2 \rightarrow \Delta Y_i) \leq p^2$ である.

以上のことから,

$$DCP_{\max}^{3n} \leq p^{3n-1} \cdot p = p^{3n}$$

$$DCP_{\max}^{3n+1} \leq p^{3n-1} \cdot p = p^{3n+1}$$

$$DCP_{\max}^{3n+2} \leq p^{3n-1} \cdot p^2 = p^{3n+1}$$

となる.

以上, (1) ~ (3) を用いることのよって,

$$DCP_{\max}^N \leq p^{3n} (N=3n, 3n+1)$$

$$DCP_{\max}^N \leq p^{3n+1} (N=3n+2)$$

が証明された.

先させる設計方針 1, MISTY 暗号のように安全を最優先させる設計方針 2, 実施例のように処理度と安全性を同程度に扱う設計方針 3 のいずれのグループに分類されていくのではないかと予される。

まとめ

本稿では、第 3 の設計方針に基づきラウンド関を検討する際に有効な新たな安全性の評価基準提案し、その有効性について重点的に考察した。の安全性評価基準を用いることによって、RC5 号と MISTY 暗号の中間に位置する設計方針、なわち、最大差分/線形確率の上界値を根拠に質的な差分解読法や線形解読法に対する証明可安全性を示すとともに、ラウンド関数の構成方法の制約が緩くなったことによって暗号化処理速のさらなる高速化を目指すことができるようになる。

今後は、この安全性評価基準を基にして具体的なラウンド関数を構成し、それを実際の暗号アルリズムに用いた場合の暗号アルリズムとしての特性や、高次の差分解読法/線形解読法やその攻撃法などに対する安全性などを調査する。

併

本研究に関連し、有益な議論ならびにアドバイをいただいたきました通信・放送機構 盛合志帆員に深く感謝いたします。また、山中喜義プロフェクトリーダーのご支援に感謝いたします。

参考文献

- [O95] 荒木志帆, 青木和麻呂, 太田和夫, “線形解読法による FEAL の最良表現探索,” 1995 年番号と情報セキュリティシンポジウム SCIS95, 14.4, 1995.
- [M97] K. Aoki, K. Kobayashi, S. Moriai, “Best Differential Characteristic Search of FEAL,”

Fourth International Workshop on Fast Software Encryption, 1997.

- [AO96] 青木和麻呂, 太田和夫, “最大平均差分確率および最大平均線形確率のより厳密な評価,” 1996 年番号と情報セキュリティシンポジウム SCIS96-4A, 1996.

- [B97] E. Biham, “A Fast New DES Implementation in Software,” *Fourth International Workshop on Fast Software Encryption*, 1997.

- [BS91] E. Biham, A. Shamir, “Differential Cryptanalysis of DES-like Cryptosystems,” *Journal of Cryptology*, Vol. 4 No. 1, pp. 3-72, 1991. (The extended abstract appeared at CRYPTO90)

- [DES] *Data Encryption Standard*, FIPS-PUB-46, (1977)

- [K96] 金子泰洋, “DES 型暗号系の証明可能安全性評価,” 「暗号アルゴリズムの設計と評価」ワークショップ, 1996.

- [LM91] X. Lai, J. L. Massey, S. Murphy, “Markov Ciphers and Differential Cryptanalysis,” *Advances in Cryptology - EUROCRYPT91*, LNCS 547, Springer-Verlag, 1991.

- [M93] M. Matsui, “Linear Cryptanalysis Method for DES Cipher,” *Advances in Cryptology - EUROCRYPT93*, LNCS 765, Springer-Verlag, 1993.

- [M94] M. Matsui, “On Correlation Between the Order of S-boxes and the Strength of DES,” *Advances in Cryptology - EUROCRYPT94*, LNCS 950, Springer-Verlag, 1994.

- [M97] M. Matsui, “New Block Encryption Algorithm MISTY,” *Fourth International Workshop on Fast Software Encryption*, 1997.

- [MAO96] S. Moriai, K. Aoki, K. Ohta, “The Best Linear Expression Search of FEAL,” *IEICE Transactions Fundamentals of Electronics, Communications and Computer Sciences*, Vol. E79-A, No. 1, pp. 2-11, 1996.

- [MKOM90] S. Miyaguchi, S. Kurihara, K. Ohta, H. Morita, “Expansion of FEAL Cipher,”

Review of Electrical Communication Laboratories, Vol. 2, No. 6, 1990

- [N94] K. Nyberg, “Linear Approximation of Block Ciphers,” *Advances in Cryptology - EUROCRYPT94*, LNCS 950, Springer-Verlag, 1994.

- [R94] R. L. Rivest, “The RC5 encryption algorithm,” *Second International Workshop on Fast Software Encryption*, LNCS1008, Springer-Verlag, 1994.

- [SM97] A. Shimizu, S. Miyaguchi, “Fast Data Encipherment Algorithm FEAL,” *Advances in Cryptology - EUROCRYPT97*, LNCS 304, Springer-Verlag, 1997.

- [SoM97] 反町亨, 松井充, “RC5 の強度評価に関する一考察 (その 3),” 1997 年暗号と情報セキュリティシンポジウム SCIS97-18A, 1997.

- [TSM97] 時田俊雄, 反町亨, 石塚裕一, 松井充, “ブロック暗号のマルチプルバスサーチに関する一考察,” 1997 年暗号と情報セキュリティシンポジウム SCIS97-24B, 1997.

Appendix A

定理 2 の $DCP_{\max}^n \leq p^*$ についてのみ証明する。

$LC P_{\max}^n \leq q^*$ についても同様に証明できる。

(1) $N = 1(n = 0)$ のとき

まず, $\Delta X_1 = (\Delta X_1^L, 0), \Delta X_1^L \neq 0$ とする。この場合、明らかに $DCP_{\max}^1 = 1$ となる。

次に, $\Delta X_1 = (\Delta X_1^L, \Delta X_1^R), \Delta X_1^R \neq 0$ とすると, $DCP_{\max}^1 \leq p$ になる。

ゆえに, $DCP_{\max}^1 \leq p^0 = 1(N = 1)$ が成り立つ。

(2) $N = 2, 3(n = 1)$ のとき

まず, $\Delta X_2^L = 0$ の場合を考える。

このとき, $\Delta X_2^L = \Delta X_2^R \neq 0$ でなければならぬので, (1) から $DCP_{\max}^2 = DCP_{\max}^1 \leq p$ となる。

さらに, $\Delta X_2^L = 0$ から $\Delta X_2^L = \Delta X_2^R \neq 0$ となるので, $DCP_{\max}^2 = DCP_{\max}^1 \cdot DP(\Delta X_2^L \rightarrow \Delta X_2^R) \leq p^2$ である。次に, $\Delta X_2^L \neq 0$ の場合を考える。

このとき, $\Delta X_1^L, \Delta Y_1^L$ の少なくとも一方は 0 ではない。また, $\Delta Y_1^L \neq 0$ であれば $\Delta X_1^L \neq 0$ である。ゆえに, $\Delta X_1^L \neq 0$ である。

さて, (1) から $\Delta X_1^L = (\Delta X_1^L, 0), \Delta X_1^L \neq 0$ のときに $DCP_{\max}^1 = 1$ で, かつ $\Delta X_2^L \neq 0$ になることが示されているので, $DCP_{\max}^2 = \max_{\Delta X_1^L, \Delta X_2^L} DP(\Delta X_2^L \rightarrow \Delta Y_2^L) \leq p$ となる。さらに, $\Delta Y_2^L = 0$ とすると $\Delta X_2^L = 0$ となり, $DCP_{\max}^2 = DCP_{\max}^1 \leq p$ である。

ゆえに, $DCP_{\max}^2 \leq p(N = 2, 3)$ が成り立つ。

(3) $N = 2n, 2n+1(n = m+1, m \geq 1)$ のとき

$DCP_{\max}^{2n} \leq p^*, DCP_{\max}^{2n+1} \leq p^*$ が成り立っていると仮定する。

この仮定より, $DP(\Delta X_{2n+1}^L \rightarrow \Delta Y_{2n+1}^L) = 1$ であり, $\Delta X_{2n+1}^L = \Delta Y_{2n+1}^L = 0$ となる。また, このとき, $DCP_{\max}^{2n}, DCP_{\max}^{2n+1}$ は以下のとおりである。

$$DCP_{\max}^{2n} = \max_{\Delta X_1^L, \Delta X_{2n+1}^L} DCP(\Delta X_{2n}^L \rightarrow \Delta Y_{2n}^L)$$

$$DCP_{\max}^{2n+1} = \max_{\Delta X_1^L, \Delta X_{2n+1}^L} \left\{ DCP_{\max}^{2n+1}, DP(\Delta X_{2n}^L \rightarrow \Delta Y_{2n}^L) \right\} \times DP(\Delta X_{2n+1}^L \rightarrow \Delta Y_{2n+1}^L)$$

ここで, $\Delta X_{2n+1}^L = 0$ であるという仮定より, $\Delta X_{2n+1}^L \neq 0$ となるので, $\Delta X_{2n}^L = \Delta X_{2n+1}^L \neq 0$ であり, $DP(\Delta X_{2n}^L \rightarrow \Delta Y_{2n}^L) \leq p$ となる。

さらに, $\Delta Y_{2n}^L = 0$ とすると, $\Delta X_{2n}^L = \Delta X_{2n+1}^L = 0$ となり, $DP(\Delta X_{2n}^L \rightarrow \Delta Y_{2n}^L) \cdot DP(\Delta X_{2n+1}^L \rightarrow \Delta Y_{2n+1}^L) \leq p$ である。

ゆえに $DCP_{\max}^{2n} \leq p^*, p = p^*, DCP_{\max}^{2n+1} \leq p^*, p = p^*$ となる。

以上, (1) ~ (3) を用いることによって, $DCP_{\max}^n \leq p^*(N = 2n, 2n+1)$ が証明された。

Appendix B

定理 3 の DCP_{\max}^n の関係についてののみ証明する。
 $LC P_{\max}^n$ の関係についても同様に証明できる。

(1) $N = 1, 2(n = 0)$ のとき

ラウンド関数が実現すべき DP_{max}, LP_{max} との関係が求まる。

そこで、筆者らは 8 段, 12 段, 16 段のいずれかを構成段数とする 64 ビット長 DES 型暗号アルゴリズムで、ラウンド関数は全単射であるものを検討対象とした。ここで、構成段数は、 $UDCP_{max}, ULCP_{max}$ が 2^{16} を初めて下回った段数に 3 段分余分に足した段数とする。すなわち、8 段の場合は 5 段目、12 段の場合は 9 段目、16 段の場合は 13 段目で 2^{16} を初めて下回ることである。ちなみに、3 段分を余分に足すのは、安全性のマーキングをとるためである。このとき、ラウンド関数が実現すべき DP_{max}, LP_{max} は表 2 のようになる。

表 2 要求される最大差分/線形特性確率

構成段数	ラウンド関数での確率	全体の確率
8	$2^{-21.3}$ 以下	$2^{-108.7}$ 以下
12	$2^{-10.7}$ 以下	$2^{-85.3}$ 以下
16	2^{-9} 以下	2^{-90} 以下

次に、高速性について考察する。なお、ここではゾフトウェアでの高速性を指す。

このとき、安全性評価を損なわずに、かつ高速性を実現するために、バイト単位の処理体系で行えるよう、データランダム化には 8 ビット長入力サイズのテーブル参照を用いた S-box を構成する。そして、これにビット演算を組み込むことによってラウンド関数を構成することにした。

5.2. 具体的なラウンド関数例

5.1 節で考察した条件を満たすようなラウンド関数を検討する。

S-box が 8 ビット長入力サイズであることから、S-box の最大差分/線形特性確率の最小値は 2^{-6} である（と予想されている）。この場合、ラウンド関数で実現できる DP_{max}, LP_{max} は、 $2^6 \cdot 2^{-12} \cdot 2^{-18} \cdot 2^{-24}$ のいずれかとなる。これと 5.1 節の安全性の条件を合わせると、12, 16 段の場合は 2^{-12} 以下、8 段の場合は 2^{-6} を実現することが必要である。

また、ラウンド関数内では、データが 4 分割さ

れていることから、少なくとも S-box が 4 つなければ $DP_{max}, LP_{max} = 2^{-6}$ とならない。また、MISTY 暗号のラウンド関数と同じようにに再帰構造をとれば、9 つの S-box で $DP_{max}, LP_{max} = 2^{-24}$ となる。これらのことから、条件を満たすようなラウンド関数の S-box の個数は 5~9 つのいずれかである。そこで、筆者らは、S-box の個数が 5~8 つの場合について、いくつかの構造を考え、 DP_{max}, LP_{max} がどのようになるかを調べた（表 3 参照）。

表 3 S-box の個数と確率の関係

個数	確率	個数	確率
5	2^{-6}	7	2^{-12}
6	2^{-12}	8	2^{-18}

この結果、我々の見解としては、S-box の個数が 5 つで $DP_{max}, LP_{max} = 2^{-12}$ を実現すること、および 8 つで $DP_{max}, LP_{max} = 2^{-18}$ を実現することには否定的である。

そこで、本稿では、まだ例が上がっていない、6 つのテーブルを用いた場合のラウンド関数例を図 6 に示す。

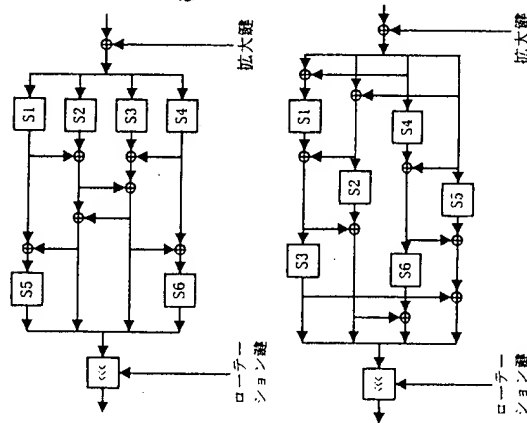


図 6 ラウンド関数例

6. 評価

6.1. 実装

図 6 のラウンド関数例の 1 つを用いて、構成段数 12 段の DES 型暗号アルゴリズムをアセンブラで実装し、その暗号化速度を測定した。測定条件は以下のとおりである。

- Pentium, 166 MHz
- WINDOWS95
- Visual C++ Ver. 4.0 (実行速度最適化)
- 32KB データを 10000 回暗号化したときの時間を測定
- 出力された暗号文を次の暗号化のための平文とした

第一版のアセンブラソースによる測定結果では、34.5Mbps を達成した。むろん、このソースは第一版であるので、さらなる改善が期待できる。

6.2. 安全性と処理速度の関係

6.1 節で実装したラウンド関数例では、 $DP_{max}, LP_{max} = 2^{-12}$ を実現しており、また構成段数が 12 段であるから、 $UDCP_{max}, ULCP_{max} = 2^{-24}$ である。ここで、差分解析法に対する安全性評価の比較のため、実装例とあわせて、RC5 暗号³⁾と MISTY 暗号についても図 7 に示す。図 7 より、実装例での $UDCP_{max}$ は、RC5 暗号の DCP_{max} よりもはるかに小さいので、オリジナルの差分解析法に対しては RC5 暗号よりも安全であると期待できる。

次に、安全性と処理速度の関係を図 8 に示す。参考までに、DES 暗号、FEAL 暗号、RC5 暗号、MISTY 暗号についても示す。なお、これらの評価資料として、[M93,AA095,AKM97,SoM97]を用いた。ただし、ここでの安全性では、DES 暗号、FEAL

³⁾ RC5 暗号は、ブロック長 2w、段数 r、鍵長 b もパラメータ化しており、正しくは RC5-w/r/b 暗号と表記する。ここでは、推奨形とされる RC5-32/12/16 暗号を用いる。また、RC5 暗号は Markov cipher ではないので、定義 4 は当てはまらない。

図 8 暗号アルゴリズムの現状と今後

ここで、興味深いのは、現在主流の方式である、DES 暗号と FEAL-32 暗号を結ぶ線が、RC5 暗号と MISTY 暗号を結ぶ線に移動する傾向にあることである。つまり、今後主流になるであろう暗号アルゴリズムは、RC5 暗号のように処理速度を最

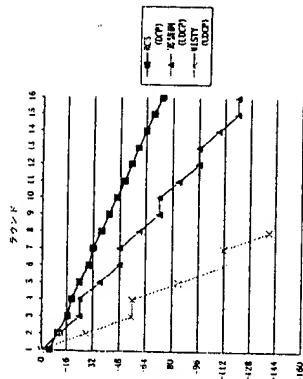
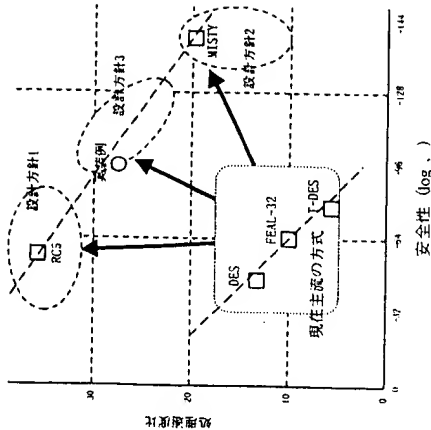


図 7 差分解析法に対する安全性比較



【定理 2】 段数 $N = 2n, 3n + 1$ の DES 型暗号アルゴリズムの場合、 $p = DP_{\max}^N, q = LP_{\max}$ とすると、 $DCP_{\max}^N, LCP_{\max}^N$ の上界値は以下のように評価される。

$$DCP_{\max}^N \leq p^* \cdot LCP_{\max}^N \leq q^*$$

【定義 5】 定理 2 のように $DCP_{\max}^N, LCP_{\max}^N$ の上界値が評価されるとき、 $UDCP_{\max}^N = p^*, ULCP_{\max}^N = q^*$ と定義する。

【定理 3】 段数 $N = 3n, 3n + 1, 3n + 2$ の DES 型暗号アルゴリズムで、ラウンド関数 F が全単射である場合、 $p = DP_{\max}^N, q = LP_{\max}$ とすると、 $DCP_{\max}^N, LCP_{\max}^N$ の上界値は以下のように評価される。

$$N = 3n, 3n + 1 \text{ のとき}$$

$$DCP_{\max}^N \leq p^* \cdot LCP_{\max}^N \leq q^*$$

$$N = 3n + 2 \text{ のとき}$$

$$DCP_{\max}^N \leq p^{2n+1} \cdot LCP_{\max}^N \leq q^{2n+1}$$

【定義 6】 定理 3 のように $DCP_{\max}^N, LCP_{\max}^N$ の上界値が評価されるとき、 $UDCP_{\max}^N, ULCP_{\max}^N$ を以下のように定義する。

$$N = 3n, 3n + 1 \text{ のとき}$$

$$UDCP_{\max}^N = p^*, ULCP_{\max}^N = q^*$$

$$N = 3n + 2 \text{ のとき}$$

$$UDCP_{\max}^N = p^{2n+1}, ULCP_{\max}^N = q^{2n+1}$$

4.2. 実験結果と考察

3.2 節で述べたように、 $UDCP_{\max}^N, ULCP_{\max}^N$ と $ADP_{\max}^N, ALP_{\max}^N$ とのあいだに安全性に関する理論的な関係はない。しかし、本来、 $ADP_{\max}^N, ALP_{\max}^N$ で安全性評価が行われるべきであることを考えれば、今回提案した $UDCP_{\max}^N, ULCP_{\max}^N$ による評価が安全性評価としてどの程度の妥当性があるものなのかを、特に $ADP_{\max}^N, ALP_{\max}^N$ による評価との大小関係を明示することによって明確にしておく必要がある。

とはいえ、暗号アルゴリズムそのものを使って

その大小関係を示すことは不可能である。そこで、ここではモデルを用いた実験を通して、3.2 節で述べた評価基準の大小関係を考察する。

今回の実験では、ブロック長 16 ビット、8 ビット入出力のラウンド関数を利用して、差分確率についての関係調べることにした。なお、ラウンド関数は全単射である。

図 3～図 5 に、 $DP_{\max}^N = 2^{-4}, 2^{-5}, 2^{-6}, 2^{-7}, 2^{-8}$ の 3 例についての実験結果を示す。なお、利用したラウンド関数は、 $DP_{\max}^N = 2^{-4}, 2^{-5}$ については、ランダムに 8 ビット入出力テーブルを生成した後、 DP_{\max}^N を検査して $DP_{\max}^N = 2^{-4}, 2^{-5}$ となったものを採用した。また、 $DP_{\max}^N = 2^{-6}$ については、 $GF(2^4)$ のべき乗関数を利用して生成した 8 ビット入出力テーブルを採用した。

まず、 ADP_{\max}^N について考える。今回の実験では、ブロック長が 16 ビットであるため、 ADP_{\max}^N は 2^{-16} に収束する [LAKSHI]。したがって、本来、安全性評価において 2^{-16} より小さい確率というのは存在しない。そこで、 2^{-16} より大きい範囲を特に注目する。

今回の 3 例において、 $UDCP_{\max}^N < ADP_{\max}^N$ となるのは、 $N \geq 5$ (図 3)、 $N \geq 6$ (図 4)、 $N \geq 5$ (図 5) のときである。しかも、図 4 の $N = 6, 7$ 、図 5 の $N = 5$ に関しては、 $UDCP_{\max}^N$ と ADP_{\max}^N との差はほとんどない。つまり、安全性評価として意味のある範囲である $UDCP_{\max}^N \geq 2^{-16}$ において、 $UDCP_{\max}^N$ は ADP_{\max}^N より大きい、少なくとも同程度であることがわかる。そして、 $UDCP_{\max}^N$ と ADP_{\max}^N との差が明確に現れるのは、 $UDCP_{\max}^N < 2^{-16}$ になった時点からである。

これに対し、 DCP_{\max}^N では、図 4 のようにつねに $DCP_{\max}^N < ADP_{\max}^N$ ($N \geq 3$) となっており、安全性評価としてはきわめて不十分となる場合がある。また、 $UADP_{\max}^N$ では、つねに $UADP_{\max}^N \geq ADP_{\max}^N$ であることが保証されるが、段数が増えれば明らかに ADP_{\max}^N とはかけ離れた値となり、実体を反映しにくくなる。

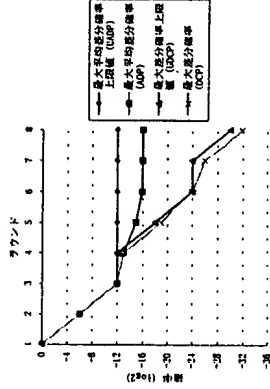


図 3 $DP_{\max}^N = 2^{-4}$ のときの差分確率変化

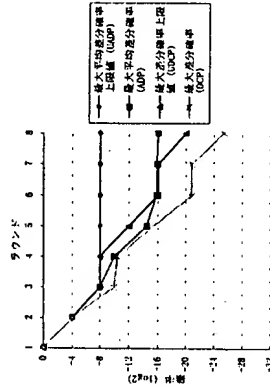


図 4 $DP_{\max}^N = 2^{-5}$ のときの差分確率変化

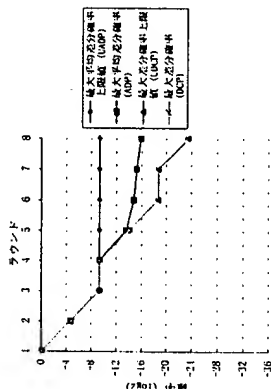


図 5 $DP_{\max}^N = 2^{-6}$ のときの差分確率変化

以上のことに、 ADP_{\max}^N が N による単純減少関数であることを考え合わせれば、 $UDCP_{\max}^N$ である程度まで確率を抑え込むことによって、実質的に安全性を確保されることが期待できる。今回の例では、3 例とも、 $UDCP_{\max}^N$ から $N = 5$ で ADP_{\max}^N が 2^{-16} より小さいことがわかる。確率 2^{-16} は図 3 の場合の $UADP_{\max}^N$ と等しいため、 $UDCP_{\max}^N$ による評価であ

っても、実質的には、 $UADP_{\max}^N$ による評価と同じである程度の安全性評価になっていると考えられる。

以上のことは、ブロック長 16 ビットでの実験結果を基に考察しているため、一般的な暗号アルゴリズムのブロック長である 64 ビット (以上) でも必ず成り立つという保証はない。しかし、DES 暗号や FEAL 暗号など多くの暗号アルゴリズムでは DCP_{\max}^N をもって安全性評価としていること、ならびに図 5 のように暗号設計としてはあまりよくない性質を有している場合であっても上記のことが成り立っていることを考えれば、 $UDCP_{\max}^N$ による評価は 64 ビット以上についても十分に安全性評価として機能するものと考えられる。少なくとも、 DCP_{\max}^N による評価よりは ADP_{\max}^N に近く、厳密な安全性評価になっているはずである。

また、差分解読法と線形解読法との双対性から、これらのことは、線形解読法についても成り立つと期待される。

5. 高速なラウンド関数の検討

5.1. 高速なラウンド関数であるための条件

「安全性」と「高速性」を同程度に重要視する設計方針とは、安全性について少なくともなんらかの数値的な証明が可能であり、その範囲内においてできるだけ高速性を図ることである。

そこで、筆者らは、安全性の評価方法としては、 $UDCP_{\max}^N, ULCP_{\max}^N$ による評価がもっとも効果的であると考えた。なぜなら、3 章および 4 章で検討したように、 $UDCP_{\max}^N, ULCP_{\max}^N$ による評価は、厳密な意味での安全性という観点からは安全性が保証されないものの、実質的には $UADP_{\max}^N, UALP_{\max}^N$ による評価や $ADP_{\max}^N, ALP_{\max}^N$ 自体による評価とそれほど変わらない評価であると期待されること、ならびに容易に求めることができるためである。

さて、 $UDCP_{\max}^N, ULCP_{\max}^N$ によって安全性を示すことにすると、暗号アルゴリズムの構成段数とラ

1. はじめに

差分解読法^[BS91]や線形解読法^[M93]に代表される、ブロック暗号に対する強力な解読法が発表されて以来、DES 暗号^[DES]を始めとする多くの暗号アルゴリズムが、これらの解読法に対する安全性評価の対象とされてきた。そして、安全性評価が進化した結果、対象となった暗号アルゴリズムの多くは、これらの解読法に対する安全性の確保と引き替えて、処理速度の高速性を犠牲にせざるを得なくなってきた。例えば、DES 暗号から Triple-DES 暗号、FEAL-8 暗号^[SM87]から FEAL-32 暗号^[DKK90]などがそうである。

このような流れを受け、近年では、これらの解読法に対する安全性と高速性とを両立させることを目的とした新しい暗号アルゴリズムの提案が相次いでいる。なかでも、RC5 暗号^[RC94]と MISTY 暗号^[M97]が代表例として挙げられる。

この二つの暗号アルゴリズムには、RC5 暗号では高速性を、MISTY 暗号では安全性をより重視した設計方針を採用した点に大きな違いがある。具体的には、RC5 暗号は、ソフトウェアでの処理速度を最重要視して算術演算を取り入れたため、DES 暗号など従来の暗号アルゴリズムと比較して 3.5 倍程度以上の高速化を実現した。しかし、未だに差分解読法や線形解読法に対する安全性が十分に評価されていない。一方、MISTY 暗号は、差分解読法や線形解読法に対する証明可能な安全性を最重要視して 7 ビットと 9 ビットを S-box の最小単位として構成したため、最大平均差分/線形確率が 2^{-56} 以下という確率を実現して差分解読法や線形解読法に対する安全性を定量的に示した。しかし、高速化の面では従来の暗号アルゴリズムと比較して 2 倍弱程度の高速化にとどまる。

そこで、筆者らは、RC5 暗号や MISTY 暗号の設計方針とは異なる第 3 の設計方針、すなわち高

速性と安全性を同程度に重視する設計方針を考へ、その設計方針に基づくラウンド関数について検討している。本稿では、第 1 回目として、高速なラウンド関数を設計する際に有効な新たな安全性評価基準を提案し、その有効性について重点的に考察する。

本稿の構成は以下のとおりである。2 章において本稿で使用する記号を定義する。次に、3 章で従来の差分/線形解読法に対する安全性評価基準についての概要を述べた後、本稿で提案する安全性評価基準の位置づけを示す。4 章では、提案する安全性評価基準の詳細を述べ、その有効性について検討する。5 章で第 3 の設計方針に基づくラウンド関数例について検討した後、6 章でその評価を行う。最後に、7 章で本稿のまとめならびに今後の課題を述べる。

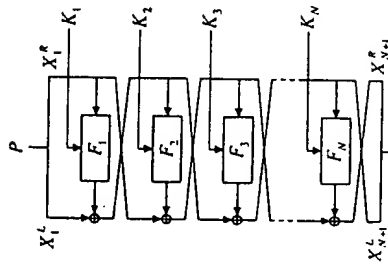
2. 準備

本稿では、以下の記号を用いる。

- $P = X_i$: 平文 (64 ビット)
- $C = X_{N+1}$: 暗号文 (64 ビット)
- F_i : 第 i 段ラウンド関数
- X_i : 第 i 段でのデータ (64 ビット)
- X_i^L, X_i^R : 第 i 段での上位、下位データ (32 ビット)
- Y_i : F_i からの出力データ (32 ビット)
- K_i : F_i への匠大鍵
- ΔX : X の差分値
- ΓX : X のマスク値
- \bullet : ビットごとの論理積に対する偶数バリティ値

また、本稿で対象とする暗号アルゴリズムは、図 1 に示すような N 段 DES 型暗号アルゴリズムとする。

¹ 最近、Bihara らによって新たな高速化手法^[BHM04]が提案されている。しかし、本稿ではすべてのモードが利用可能なインプリメントを対象としたため、Bihara の手法は考えない。



$$Y_i = F_i(X_i^L, K_i) = f(E(X_i^L) \oplus K_i)$$

$$X_{i+1}^L = X_i^R \oplus Y_i$$

$$X_{i+1}^R = X_i^L$$

ここで、 f は S-box などの非線形変換関数を含む変換関数、 E は線形変換関数を表す。

図 1 DES 型暗号アルゴリズム

3. 差分/線形解読法に対する安全性評価

3.1. 従来の評価基準

差分解読法や線形解読法に対する安全性の評価指標として一般に利用されるものに、「最大差分/線形確率」と「最大平均差分/線形確率」とがある。この二つの確率の差は、平文の差分値（暗号文のマスク値）と暗号文の差分値（平文のマスク値）が与えられたときに、ブロック暗号内部で推移していく差分値（マスク値）の変化を一意に決めたうえでの単一経路（Single path）における評価であるか、それらの変化をすべて考慮に入れた、いわゆる多重経路（Multiple paths）における評価であるかの違いによる。

【定義 1】 差分特性確率 $DP(\Delta X_i^* \rightarrow \Delta Y_i)$ および線形特性確率 $LP(\Gamma Y_i \rightarrow \Gamma X_i^*)$ を以下のよう

$$DP(\Delta X_i^* \rightarrow \Delta Y_i) = P_{Y_i}[F_i(X_i^*) \oplus F_i(X_i^* \oplus \Delta X_i^*) = \Delta Y_i]$$

$$LP(\Gamma Y_i \rightarrow \Gamma X_i^*) = \left| P_{Y_i}[X_i^* \cdot \Gamma X_i^* = Y_i \cdot \Gamma Y_i] - \frac{1}{2} \right|$$

【定義 2】 最大差分特性確率 DP_{\max} および最大線形特性確率 LP_{\max} を以下のよう

$$DP_{\max} = \max_{\Delta X_i^* \neq \Delta Y_i} DP(\Delta X_i^* \rightarrow \Delta Y_i)$$

$$LP_{\max} = \max_{\Gamma Y_i \neq \Gamma X_i^*} LP(\Gamma Y_i \rightarrow \Gamma X_i^*)$$

【定義 3】 最大差分確率 DCP_{\max} および最大線形確率 LCP_{\max} を以下のよう

$$DCP_{\max} = \max_{\Delta X_i^* \neq \Delta Y_i} \sum_{Y_i \in \mathcal{Y}} DP(\Delta X_i^* \rightarrow \Delta Y_i)$$

$$LCP_{\max} = \max_{\Gamma Y_i \neq \Gamma X_i^*} \sum_{Y_i \in \mathcal{Y}} LP(\Gamma Y_i \rightarrow \Gamma X_i^*)$$

【定義 4】 最大平均差分確率 ADP_{\max} および最大平均線形確率 ALP_{\max} を以下のよう

$$ADP_{\max} = \max_{\Delta X_i^* \neq \Delta Y_i} \sum_{Y_i \in \mathcal{Y}} DP(\Delta X_i^* \rightarrow \Delta Y_i)$$

$$ALP_{\max} = \max_{\Gamma Y_i \neq \Gamma X_i^*} \sum_{Y_i \in \mathcal{Y}} LP(\Gamma Y_i \rightarrow \Gamma X_i^*)$$

定義から明らかなように $DCP_{\max} \leq ADP_{\max}$ 、 $LCP_{\max} \leq ALP_{\max}$ であり、また差分解読法や線形解読法に対する安全性は確率の最大値によって評価できることから、より厳密に安全性評価を行うならば、多重経路を考慮している ADP_{\max} 、 ALP_{\max} で評価を行うべきであるとされている^[LMN91, N94]。

しかし、今のところ、 ADP_{\max} 、 ALP_{\max} を求めることは現実的には不可能であるため、その理論的上界で評価する方法しかない。例えば DES 型暗号

² このように定義される場合、対象となる暗号アルゴリズムが Markov cipher^[LMN91]であることを前提にしている。したがって、本稿でも Markov cipher であるものについて後述の対象とする。

表 1 評価基準の特徴

	安全性 評価	段数 依存性	計算 容易性	評価 実績
1 ADP_{max}^N, ALP_{max}^N	◎	○	×	なし
2 $UADP_{max}^N, UALP_{max}^N$	◎	×	○	MISTY
3 DCP_{max}^N, LCP_{max}^N	○	○	△	DES, FEAL etc.
4 $UDCP_{max}^N, ULCP_{max}^N$	○	○	○	なし

評価基準(2)による評価は、求められる評価値が ADP_{max}^N, ALP_{max}^N より小さくなることはないという点で、安全性評価としては十分である。しかし、欠点として、 ADP_{max}^N, ALP_{max}^N の段数依存性がほとんど反映されないことが挙げられる。つまり、定理 1 からは、 ADP_{max}^N, ALP_{max}^N がおよそ DP_{max}, LP_{max} の平方以下であるということしか証明されず、 N に依存して ADP_{max}^N, ALP_{max}^N がどのように変化するかという点については何も言及されない。

このことは、 DP_{max}, LP_{max} が大きい代わりに N も大きくすることによって安全性を確保しようとする暗号アルゴリズムにはほとんど適用できないことを意味している。なぜなら、このようなアルゴリズムで N をある程度以上大きくすることによって、実際には ADP_{max}^N, ALP_{max}^N を十分に小さくし、安全であるように設計されているとしても、評価上は ADP_{max}^N, ALP_{max}^N が十分に小さいと想定させるような情報は提供しないからである⁴。このため、MISTY 暗号のようにもともと上界値が小さい暗号では差分解読法や線形解読法に対して安全であるとはいっても、上界値が小さくならない暗号では差分解読法や線形解読法に対して安全であるとも安全でないともいえない。

しかし、現状では、多くの暗号アルゴリズムは $N \rightarrow \infty$ とすれば ADP_{max}^N, ALP_{max}^N の分布が一樣分布になることは示されている^(MORSE)。しかし、 N を特定したときに ADP_{max}^N, ALP_{max}^N の分布がどのようなものになっているかはわからない。

の場合、4 段以上であれば、 DP_{max}, LP_{max} の平方以下に漸近していくことが示されている。

【定理 1】^(MORSE) $p = DP_{max}, q = LP_{max}$ とすると、 ADP_{max}^N, ALP_{max}^N の上界値は以下のとおりに評価される³。

$$4,5 \text{ 段: } ADP_{max}^{4,5} \leq 2p^2, ALP_{max}^{4,5} \leq 2q^2$$

$$6,7 \text{ 段: } ADP_{max}^{6,7} \leq p^2 + 2p^3, ALP_{max}^{6,7} \leq q^2 + 2q^3$$

$$8,9 \text{ 段: } ADP_{max}^{8,9} \leq p^2 + p^3 + 2p^4$$

$$ALP_{max}^{8,9} \leq q^2 + q^3 + 2q^4$$

3.2. 安全性に対する設計方針

3.1 節で述べたように、厳密な意味での差分解読法や線形解読法に対する安全性は、 ADP_{max}^N, ALP_{max}^N で評価される (評価基準(1))。したがって、もし ADP_{max}^N, ALP_{max}^N を実際に求めることができるのなら、これ以上正確な安全性評価基準はない。しかし、今のところ ADP_{max}^N, ALP_{max}^N を求めることは現実的に不可能である。このため、これらの確率に代わる何らかの評価基準が必要となるとくる。

そこで、今までよく利用されている評価基準が以下の 2 つである。

- 評価基準(2): ADP_{max}^N, ALP_{max}^N の理論的上界値による評価。
以下、この評価値を $UADP_{max}^N, UALP_{max}^N$ と表す。
- 評価基準(3): DCP_{max}^N, LCP_{max}^N による評価

この 2 つの評価基準に加えて、本稿では、新たに評価基準(4)として、 DCP_{max}^N, LCP_{max}^N の上界値による評価を提案する。以下、この評価値を $UDCP_{max}^N, ULCP_{max}^N$ と表す。

これらの評価基準について、以下にその説明をするが、始めに表 1 にそれぞれの評価基準の特徴をまとめておく。

3 ラウンド関数が全単射である場合は、3 段以上であれば、 $ADP_{max}^N \leq p^2, ALP_{max}^N \leq q^2$ である^(MORSE)。

もともと設計された段数をもって安全性を確保するように設計されているのであって、必ずしも DP_{max}, LP_{max} が小さくなるように設計されているわけではない。

評価基準(3)による評価は、単一経路しか想定しないという制限が付けられるものの、評価を行うための汎用的な探索アルゴリズムがすでに提案されており、実際に DES 暗号や FEAL 暗号などに適用されている^(MORSE, MORSE, MORSE)。この評価基準のメリットとしては、段数依存性が反映されることと、ほぼ同一条件下の確定的な値として評価されるために複数の暗号アルゴリズム間の安全性について大まかな比較などができることである。また、安全性評価に関しては、差分解読法や線形解読法で実際に解読を行う場合、今のところ DCP_{max}^N, LCP_{max}^N となる場合の経路が解読に用いられることから、評価基準(3)による評価でも実用的には十分であると考えられている。

しかし、評価基準(3)の欠点としては 2 つある。まず 1 つは、理論的にいえば、評価基準(3)による評価は ADP_{max}^N, ALP_{max}^N の下限を示しているにすぎず、厳密な安全性評価とはいえない。そこで、少しでも ADP_{max}^N, ALP_{max}^N に近づける評価にするため、 DCP_{max}^N, LCP_{max}^N となる経路だけでなく、それに関連する経路についても考慮するように制限を緩めた時田らの探索アルゴリズム^(MSING97)もある。

もう 1 つは、計算機実験によって DCP_{max}^N, LCP_{max}^N を求めるため、実際にその値が得られるまでに時間がかる点である。実際には、この所用時間が短くするためにさまざまな対策を取っており、なかでも重要な対策が、特性確率をもとに不要な探索の枝刈りをいかに効率よく行うかということである。しかし、始めから差分解読や線形解読に対して安全であるように設計された暗号アルゴリズムは、同じ特性確率をもつ枝が数多く存在することにつながるため、探索数が膨大になる可能性が高い。このため、今後提案されてくる暗号アルゴリズムの多くについて、 DCP_{max}^N, LCP_{max}^N が得られるまでに長時間を有するようになる可能性が

わめて高く、評価基準(3)による評価も現実には適用困難になっていくと予想できる。

今回提案する評価基準(4)についての詳細ならびに有効性の検討は 4 章で述べるが、特徴だけをまとめると以下のとおりである。

- 容易に求まる
- 段数依存性がある
- DCP_{max}^N, LCP_{max}^N より大きい
- ADP_{max}^N, ALP_{max}^N との大小関係は不明

評価基準(4)による評価でも、 ADP_{max}^N, ALP_{max}^N との関係を示しているわけではないので、厳密な意味での安全性を証明するものではない(ただし、4.2 節で ADP_{max}^N, ALP_{max}^N との関係を検討する)。しかし、実用的な安全性評価とされている DCP_{max}^N, LCP_{max}^N よりは大きいことが保証されていることから、少なくとも実用的な安全性評価として利用しても差し支えない。また、段数依存性があり、容易に求められることから、評価基準(3)より汎用性も高い。最後に、本稿のまとめとして、以上に挙げた評価基準による評価値の大小関係を図 2 に示す。

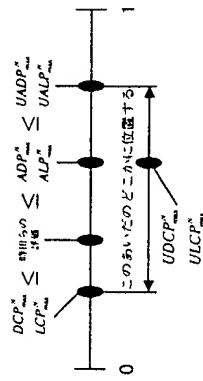


図 2 確率の大小関係

4. 最大差分/線形確率の上界値による評価手法の提案

4.1. 提案する評価基準

本稿では、より簡単な評価基準として、 DCP_{max}^N, LCP_{max}^N の上界値による評価を提案する。なお、定理の証明は Appendix につける。

少数の S-box を用いたラウンド関数の構成について (その 1)

神田 雅透[†] 高嶋 洋一[†] 松本 勉[‡]

[†] NTT ヒューマンインタフェース研究所
〒239 神奈川県横浜須賀野光の丘 1-1
{kanda.yoh}@mistral.hil.ntt.co.jp

[‡] 横浜国立大学大学院 工学研究科 人工環境システム学専攻
〒240 神奈川県横浜市保土ヶ谷区常盤台 79-5
tsutomu@mlab.dnj.ynu.ac.jp

あらまし 本稿では、高速なラウンド関数を設計する際に有効な新たな安全性評価基準を提案し、その有効性について重点的に考察する。この安全性評価基準は、理論的安全性を示すものではないが実効的には最大差分/線形確率による評価よりもはるかに厳しい基準である一方で、最大平均差分/線形確率による評価よりも実体に即した基準でもある。このため、少数の S-box しか用いないで構成されたラウンド関数であっても、十分な安全性を有していることを示しながら、高速化を目指すという第三の設計方針がとれるようになる。

さらに、この第三の設計方針に基づいたラウンド関数の例についても考察する。

キーワード ブロック暗号, 暗号設計, 差分解読法, 線形解読法, 証明可能安全性, 安全性評価基準

A round function structure consisting of few S-boxes (Part I)

Masayuki KANDA[†] Youichi TAKASHIMA[†] Tsutomu Matsumoto[‡]

[†] NTT Human Interface Laboratories
1-1 Hikarino-oka Yokosuka-shi Kanagawa 239, Japan
{kanda.yoh}@mistral.hil.ntt.co.jp

[‡] Division of Artificial Environment Systems
Yokohama National University
79-5 Tokiwadai Hodogaya-ku Yokohama-shi Kanagawa 240, Japan
tsutomu@mlab.dnj.ynu.ac.jp

Abstract

In this paper, we propose a new security evaluation against differential/linear cryptanalysis, and discuss its effectiveness. This evaluation is very useful for designing secure encryption algorithms. It can provide more practical criterion than the maximum average of differential/linear probability, and more secure criterion than the differential/linear characteristic probability. According to the evaluation, it comes out the possibility of another structure of encryption algorithms even if it is an easy implementation for high-speed to diminish the number of S-boxes.

And, we present examples of round function which is designed under above design policy.

key words Block cipher, Design, Differential cryptanalysis, Linear cryptanalysis,
Provably secure, Security criterion

信



電子情報通信学会技術研究報告

ISEC 97 - 14 ~ 22

(情報セキュリティ)

1997年7月18日

EIC 社団法人 電子情報通信学会

